История успеха

СОЗДАНИЕ БЕЗОПАСНОЙ ЭКОСИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ:

Совместный опыт Group-IB
и «Мобильная карта»

ПЕРВЫЙ ЦУПИС

group-ib.ru

2,7 млн
зарегистрированных клиентов

>200 тыс.
платежей ежедневно

9
букмекерских компаний подключено

Год основания:
2013

Отрасль:
ФИНАНСЫ

Деятельность:
УЧЕТ ПЕРЕВОДОВ ИНТЕРАКТИВНЫХ СТАВОК МЕЖДУ ИГРОКОМ И БУКМЕКЕРСКОЙ КОМПАНИЕЙ

Количество сотрудников:
> 130

«Мобильная карта» (Лицензия Банка России № 3522-К) реализует на российском рынке масштабный проект «ПЕРВЫЙ ЦУПИС» (Центр учета переводов интерактивных ставок) для букмекерских контор, который развивает экосистему электронных платежей для любителей спортивных ставок, добиваясь роста национального букмекерского рынка с учетом интересов государства и общества.

Проект помогает достичь финансовой прозрачности и взаимного доверия между букмекером, игроком и регулятором. Для поддержки клиентов и букмекеров функционирует круглосуточная служба поддержки, которая доступна по всем каналам связи и обрабатывает свыше 30 000 сообщений в месяц.

Среди партнеров «ПЕРВОГО ЦУПИС» — крупнейшие российские букмекерские компании: «Лига Ставок», 1хСтавка, Winline, BETCITY, Parimatch и другие.

ПЕРВЫЙ ЦУПИС

Описание ситуации

Сфера финансов, в которой работает «ПЕРВЫЙ ЦУПИС», постоянно подвержена различным киберугрозам. Это могут быть целевые атаки на финансовые организации, атаки на основе социальной инженерии и другие киберугрозы.

Рост популярности проекта «ПЕРВЫЙ ЦУПИС» и его партнеров также является фактором риска. Более 2,7 млн. зарегистрированных клиентов доверяют компании данные своих платежных карт и персональные данные. Ежедневно через сервис проходит более 200 000 платежей, а во время мировых спортивных событий (например, Чемпионата мира по футболу FIFA 2018) их количество в пиковые периоды могло превышать 1200 платежей в минуту.

Именно поэтому «Мобильная карта» уделяет пристальное внимание неприкосновенности персональных данных, чтобы не допустить их кражу с целью выкупа и другие инциденты. Для поддержания необходимого уровня информационной безопасности компания регулярно проводит комплексную проверку своей инфраструктуры как собственными силами, так и с помощью независимых экспертов.

«Мобильная карта» обратилась к Group-IB за комплексом услуг, которые позволили бы проверить защищенность информационной системы и готовность организации к реагированию на киберинциденты, а также повысить осведомленность сотрудников в вопросах кибербезопасности.

> **Почему выбрали Group-IB?**
>
> Group-IB – это, пожалуй, лидер на российском рынке по расследованию киберинцидентов. Ваш большой опыт и наработанные практики помогли качественно оценить нашу инфраструктуру, процессы и сотрудников.
>
> **Сергей Гуляев,**
> директор по информационным технологиям и безопасности «Мобильная карта»

Решение Group-IB

На протяжении годового сотрудничества «Мобильная карта» с Group-IB были оказаны следующие услуги для комплексной проверки инфраструктуры и повышения осведомленности сотрудников.

I. Тестирование на проникновение

На этапе тестирования специалисты Group-IB:

- Выполнили поиск уязвимостей в программно-аппаратном окружении доступных сетевых узлов внешнего сетевого периметра;
- Провели эксплуатацию обнаруженных уязвимостей, чтобы оценить их уровень риска;
- Составили описания всех уязвимостей;
- Разработали рекомендации по их устранению.

II. Pre-IR Assessment

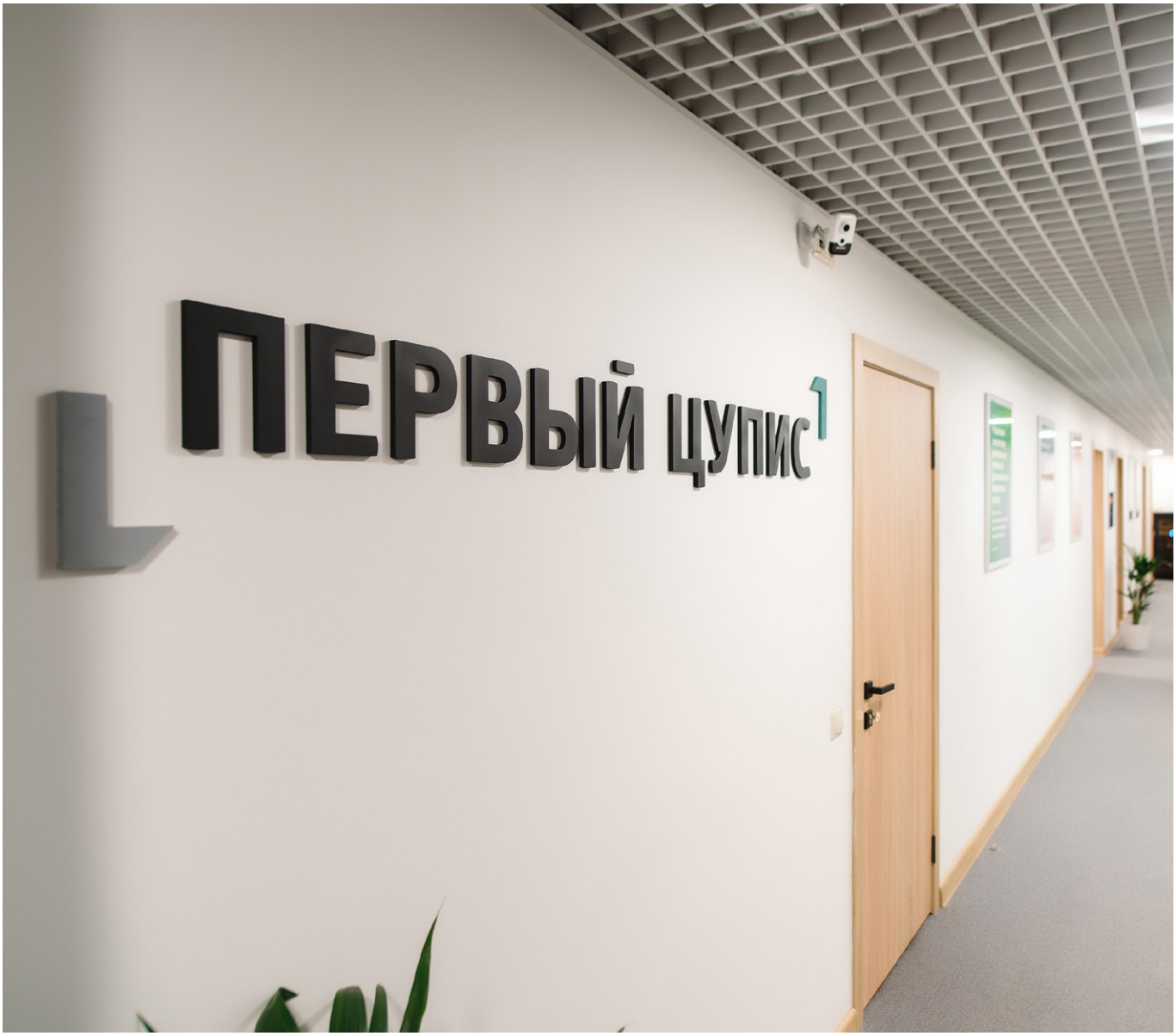
В ходе уникальной для российского рынка с точки зрения состава работ услуги по проверке готовности к реагированию на киберинциденты специалистами Лаборатории компьютерной криминалистики Group-IB были успешно выполнены все три ее этапа:

- Проверка сетевой и системной инфраструктуры на предмет готовности к реагированию на инциденты информационной безопасности;
- Проведение расширенного интенсивного тренинга для технических специалистов «Мобильная карта» по реагированию на киберинциденты;
- Проверка готовности организационной структуры к инцидентам и создание инструкций для специалистов по реагированию.

III. Обучающие курсы по кибербезопасности

При реализации обучающего комплекса для сотрудников «Мобильная карта» удалось охватить все департаменты компании и провести обучение в соответствии с потребностями каждого из них.

- **Для всех сотрудников компании (топ-менеджмента, HR, бухгалтерии и других отделов)** был проведен мастер-класс «Цифровая гигиена». На мастер-классе были рассмотрены правила безопасности корпоративных и личных устройств, создания и хранения безопасных паролей, безопасности в мессенджерах и социальных сетях, чтобы повысить уровень осведомленности сотрудников о возможных угрозах.
- **Для специалистов по ИБ, ИТ, сетевых инженеров и других технических направлений** были проведены мастер-классы «Тенденции высокотехнологичных преступлений» и «Имитация атаки на примере группировки Cobalt». Тренеры Group-IB рассказали об инструментах киберпреступников и об особенностях кибератак на финансовые организации, а также на примере тактик и техник, используемых группировкой Cobalt, продемонстрировали, как распознать подозрительную активность.
- **Для сотрудников, работающих непосредственно в сфере информационной безопасности**, практикующие эксперты Group-IB провели двухдневные технические обучающие курсы по компьютерной криминалистике, на которых слушатели изучили темы Memory Forensics и Windows Forensics.



Что получила «Мобильная карта»?

- Отчет, описывающий угрозы технической защищённости информационных систем в «Мобильная карта» и способы их нейтрализации;
- Отчет о проверке готовности инфраструктуры ИБ к реагированию на киберинциденты;
- Рекомендации по улучшению организационной структуры команды реагирования;
- Инструкции по реагированию на типовые инциденты ИБ (список типовых инцидентов был сформирован Лабораторией компьютерной криминалистики и исследования вредоносного кода Group-IB);
- Сертификаты для слушателей о прохождении практических обучающих курсов Group-IB.

> Нам был важен профессионализм и опыт в расследовании киберпреступлений, информация от тренера из первых рук. Нужны были профессионалы, которые бы на реальных примерах могли показать, как кредитные организации подвергаются атакам и борются с ними. В итоге общий уровень грамотности и вовлеченности в процессы безопасности компании повысился. Цель была достигнута.
>
> **Сергей Гуляев,**
> директор по информационным технологиям и безопасности «Мобильная карта»

Результат и перспектива

Благодаря эффективному сотрудничеству «Мобильная карта» и Group-IB удалось:

- Провести независимую проверку инфраструктуры и выявить в системе незначительные технические уязвимости;
- Организовать процесс управления уязвимостями в компании;
- Оценить уровень готовности компании к реагированию на киберинциденты как высокий;
- Начать реализацию рекомендаций, описанных в отчете: увеличение глубины журналирования событий ИБ, отработка ряда необходимых процедур и другое;
- Начать применение инструкций по реагированию на типовые инциденты ИБ и рекомендаций по улучшению структуры команды реагирования;
- Обучить 40 сотрудников компании «Мобильная карта»;
- Повысить уровень осведомленности и вовлеченности сотрудников компании в процессы информационной безопасности, а также дать практические навыки по реагированию на инциденты и компьютерной криминалистике техническим специалистам компании.

В дальнейшем практикующие специалисты Group-IB проведут несколько обучающих курсов для технических сотрудников заказчика, посвященных компьютерной криминалистике и Linux-инфраструктуре.

Кроме того, запланировано повторное тестирование на проникновение, а также Red Teaming (имитация целевых атак для поддержания и развития навыков выявления деструктивных воздействий и противодействия им) и Compromise Assessment (выявление следов компрометации и признаков подготовки к хакерской атаке), что в комплексе поможет проекту «ПЕРВЫЙ ЦУПИС» и дальше оставаться надежным сервисом для перевода интерактивных ставок, которому доверяют свою безопасность клиенты и партнеры.

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты интеллектуальной собственности в сети.

По версии **Gartner, IDC и Forrester,** Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, в базе которой хранится 100 000+ профайлов киберпреступников.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.

60 000+
часов реагирования

1000+
успешных расследований по всему миру

EUROPOL INTERPOL **Официальный партнер**

OSCE **Рекомендована Организацией по Безопасности и Сотрудничеству в Европе (ОБСЕ)**

Узнайте больше об обучающих курсах по кибербезопасности и других услугах Лаборатории компьютерной криминалистики Group-IB

www.group-ib.ru/cyber-education
education@group-ib.com